European Journal of
Technology
(EJT)

Comparative Analysis of Encryption Algorithms

Agbelusi Olutola and Matthew Olumuyiwa

European Journal of Technology
ISSN 2520-0712 (online)
Vol.7, Issue 1, pp 1 - 9, 2023

www.ajpojournals.org

Comparative Analysis of Encryption Algorithms

Agbelusi Olutola[1] and Matthew Olumuyiwa[2]

[1]Computer Science Department, Rufus Giwa Polytechnic, Owo

[2]School of Computing, University of Portsmouth, United Kingdom

Emails: tola52001@yahoo.com, olumuyiwa.matthew@port.ac.uk

Abstract

Purpose: Encryption algorithm allows users to extend the assurance found in the physical world to the electronic world in the carrying out of our day-to-day activities. This research attempts to make a comparative evaluation of two encryption algorithms (Advanced Encryption Standard (AES) and Rivest Shamir Algorithm (RSA) in order to ascertain the most reliable in terms of their encryption time, decryption time, Key length, and cipher length.

Methodology: Java programming was used for the development and Mongo Db to generate data parsing.

Findings: The results obtained from the development revealed that AES is considered more efficient because it uses lesser time for encryption and decryption, reduces cipher and key length as compared with RSA which consumes longer encryption and decryption time, and increases cipher and key length. Excel package was also used to display the pictorial representation of the comparison between these algorithms.

Recommendation: Advanced encryption standard is recommended for security-based application developers because of the small time of encryption and decryption.

Keywords: *Cipher Length, Encryption, Decryption, Advanced Encryption Standard (AES) and Rivest Shamir Algorithm (RSA) and Algorithm.*

1.0 INTRODUCTION

Data security is a very challenging issue that touches many areas including health and communications. There are a lot of cyber breaches (like illegal access, unauthorized individual, manipulations,destruction, or vulnerabilities) every day that has destroyed many lives as a result of not using appropriate/efficient system security mechanism (Cheng-K, 2015). This shortfall made the researchers to work on the comparative evaluation of encryption algorithms (Advanced Encryption Standard (AES) and Rivest Shamir Algorithm (RSA) in order to ascertain the more reliable one.

2.0 LITERATURE REVIEW

Nureni and Sayyidina (2018) compared (Rivest Shamir Adleman (RSA), Advanced Encryption Standard (AES), and Data Encryption Standard (DES) with the aim of considering the best in terms of reliability, dependability, and functionality. The implementation of the system was carried out with both java crypto and java security packages which enable several security features such as authorization, authentication, decryption, and encryption. In the study, audio and video files of different sizes were considered for the empirical evaluation of these algorithms as input files for the encryption process. The result showed that AES is the best among the three algorithms under the same condition. The limitation of this work is that the algorithms were not used for mobile health application.

Mansoor *et al*. (2013) based their research on the comparative analysis of different existing symmetric cryptographic algorithms for both secured wired / wireless communication. The performance (in form of weakness and strength) of the most popular symmetric algorithms in terms of authentication, flexibility, reliability, robustness, scalability, and security was looked into. The result of this analysis shows that all the algorithms were capable of securing data but most of them have an exchange between their memory usage and encryption performance except for AES which is the best among all the symmetric algorithms considered in terms of security, flexibility, memory usage, and encryption performance.

Singh and Supriya (2013) evaluated of four encryption algorithms (RSA, DES, 3DES, and AES). The research was justified by the fact that some of the existing work on the encryption algorithms are real-time and that each of the techniques is special and unique in its own way which are definitely applicable to different applications. The outcome of the project revealed that the AES algorithm is the most efficient and suitable in terms of speed, throughput, and time as well as avalanche effect. In this research, factor like cipher length and key length were not considered.

Seth *et al*. (2011) conducted research on the comparative evaluation of RSA, DES, and AES in terms of their memory usage, output byte, and computation time which is regarded as a major bottleneck in nearly all encryption algorithms. The result reveals that all the encryption algorithms have the capability of securing data. DES encryption algorithm consumes the lowest time for encryption while the AES encryption algorithm consumes the lowest memory usage. Finally, it was established that RSA takes the longest encryption time as well as memory usage and has the least output byte. Speed in terms of encryption and decryption time were not put into consideration. The researchers evaluated common encryption algorithms (DES, 3DES, RC2, Blowfish, and RC6) in terms of the encryption/decryption speed, different sizes of data blocks, different data types, and different key sizes with the mind of adopting one. The investigational

result shows that there is not much difference when the results are shown in base 64 encoding or hexadecimal base encoding. RC6 requires less time when compared to all encryption algorithms except Blowfish. The result of this research reveals that Blowfish, RC6, and RC2 have merit over other algorithms with respect to time consumption (Elminaam *et al*., 2008). This research was not used for the security of health application.

Pavithra *et al*. (2012) conducted a performance evaluation of different encryption techniques (Blowfish, AES, and DES) and considered time as their main metric. Different video files formats such as. DAT and .vob were considered with various sizes for the experimentation in order to establish the processing speed of each algorithm. The experimental results reveal that an AES algorithm is the best in terms of throughput level and processing time. In this research, factor like cipher length and key length were not considered. Adolf et al (2014) worked on a comparative analysis of AES, RC4, and Blowfish algorithms in terms of encryption time, decryption time, memory utilization, and throughput at different settings like variable key size and variable data packet size. A simulation program is developed using PHP and JavaScript scripting languages. The program encrypts and decrypts different file sizes ranging from 1MB to 50MB and the result shows that AES gives a better *solution than* all the investigated encryption techniques. This research was not used for the security of health application.

Mandal *et al*. (2012) compared advanced encryption standard (AES) and data encryption standard (DES) using avalanche effect, memory requirement as well as simulation time as metrics for both algorithms. The result showed that AES has a very high avalanche effect and reduced simulation time as compared with the DES algorithm. This implies that AES is basically useful for message encryption. This research was not used for the security of health application. Encryption and decryption time including cipher length and key length were not considered in this research. Meena and Komathi (2016) worked on different symmetric key cryptographic algorithms and analyzed various file features (data size, key size, and analyzed the variation of encryption time, decryption time, and throughput time). The simulated result revealed that encryption and decryption time does not depend upon data type but only depends upon the number of bytes present in the file. This research was not used for the security of health application.

3.0 METHODOLOGY

Two encryption techniques were compared in terms of their encryption time, decryption time, key length and cipher length.

3.1 Advance Encryption Standards Algorithm (AES)

Data security is a very important aspect of our day-to-day activities, especially in the area of health information. Stigmatization and suicidal acts could be controlled if an efficient mechanism for data security is put in place. The advanced encryption standard belongs to the family of symmetric cipher and comprises three block ciphers, AES-128, AES-192, and AES-256. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. The block size has a maximum of 256 bits, but the key size has no theoretical maximum. The cipher uses a number of encryption rounds that converts plain text to cipher text. The output of each round is the input to the next round. The output of the final round is the encrypted plain text known as cipher text. The input given by the user is entered in a matrix known as state matrix.

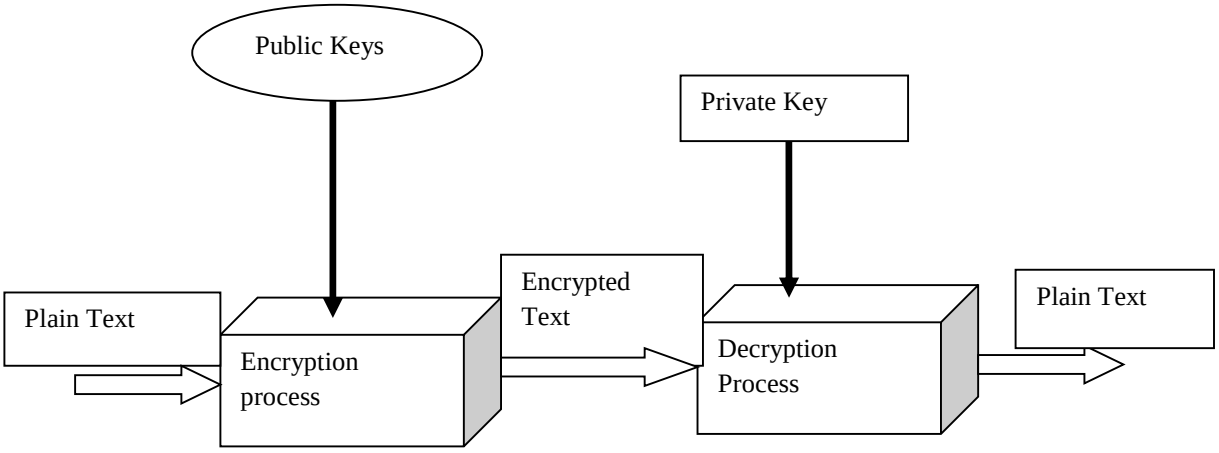

Figure 1: Encryption and decryption algorithm process of AES

3.2 Rivest Shamir Algorithm (RSA)

Rivest Shamir Algorithm is a public key algorithm invented in 1977 that support encryption and digital signatures. It is the most widely used public key algorithm which gets its security from integer factorization problem. It is simple and relatively simple to understand and implement. RSA computation occurs integers modulo n = p*q. It requires keys of at least 1024 bits for good security. Keys of size 2048 bit provide the best security. RSA algorithm is used to encrypt the data to provide security so that only the concerned user can access it.

4.0 RESULT OF THE STUDY

4.1 Comparative Analysis of Advance Encryption Standard and Rivest-Shamir-Adleman Algorithm

Advanced encryption standards and the Rivest-Shamir-Adleman algorithm were used on some data and compared in terms of the cipher length, key length, and encryption/decryption time in order to implement the technique that is suitable for this system. It was discovered that AES gives a better solution. The results are shown in tables 1 and 2.

4.2 Result of the Advanced Encryption Standard

Advanced Encryption Standard algorithms were analyzed based on their encryption time, decryption time, cipher length, and key length. It was discovered that AES gives a better solution. The output of advanced encryption standards on some data is shown in table 1.

Table 1: Result of AES

Plain Text	Cipher Text	Cipher Text	Key Length	Encryption Time	Decryption Time
I have Malaria	nvTCcMDzZCHe+dUmThGRLg==	45	25	1ms	1ms
I have Hypertension	L50ACVGT6F0GDG8GWKKHCwymwqZakXH5M1R7Jxb2ehM=	25	25	1ms	2ms
I have Headache	LcYdC03M5lUCpMDUAX9Hhw==	25	25	10ms	2ms
How are you	4BhkYZG6fM+zkeExcx6krQ==	65	25	1ms	1ms
My doctor said I should go for medical Test	YfBUO3opWr7faPNMcY3782Ee72ER7==PQdBtTd4NyWw==mzzg8Nmjwp7eGa6NBbtv4XuXIqaoMxfx/NH==	25	25	1ms	1ms
My breast is paining me	MDaDoxXXaQrxF11Hdsj/dwkGse7lO5T2UPVpQif1Duk==	45	25	1ms	1ms
I didn't sleep at night	Wn9hugfSMcmnitKHkGEewPB1msSjPdtMNhJWl4ujBU9s ==	45	25	1ms	1ms
Raches is on my body	+OGW5v6cOaxw8tlwYrAXx2bRvrumptpOJwyaq9z8bWs==	45	25	7ms	2ms
My Stomach is making noise	HFEcGbgudOQQyzCvbaFHnaOhPQdBtTd4NyWw==	45	25	1ms	2ms

The output of the Rivest-Shamir-Adleman Algorithm on some data is shown in table 2.

Table 2: Result from Rivest-Shamir-Adleman Algorithm

Plain Text	Cipher Text	Cipher Text	Key Length	Encryption Time	Decryption Time
I have Malaria	326275648852278162567 41660710011247033541 5948504956528190195385 467918088998602559624 26748836052139534369	166	1	613ms	230ms
I have Hypertension	433694726797336687726 493702311597064419941 384755329138782545541 503986827868043004781 366002521173586940466 231870049916509344320 1204077368==	136	1	50ms	379ms
I have Headache	5473997036334822809942 207475461895175512696 967217184949710496160 970776218640715745717 781056258553685640412 5	107	1	717ms	397ms
How are you	6715088703533054550461 220796080951283169083 578524782603960023493 3243415680333==	378	1	380ms	332ms
My doctor said I should go for medical Test	377977509990958635221 641640131672175717819 902295876590693923149 726717494249833488050 806745781777670860033 802663726503285900582 461922312275948890463 973622228175193279033 975501498480226656658 911594080434066170041 551735958103551310114 922225691901496394144 897206492020556636713 024004517962813693806 201972948768951==	308	1	637ms	292ms

The cipher length, key length, encryption time, and decryption time for AES is lesser than that of RSA which is very good for real time application as shown in table 3.

Table 3: Comparison table of AES and RSA encryption techniques

	AES	RSA
Cipher Length	Less	More
Key Length	Less	More
Encryption time	Less	More
Decryption Time	Less	More

The comparison of AES and RSA in terms of cipher length, encryption time and decryption time respectively is shown in figure 2, 3, and 4. The cipher length of RSA is higher than that produced by AES. Figure 3 and 4 shows that a very small time is required for a message to encrypt and decrypt and as a result increasing the performance of the application in terms of period of completion of task.

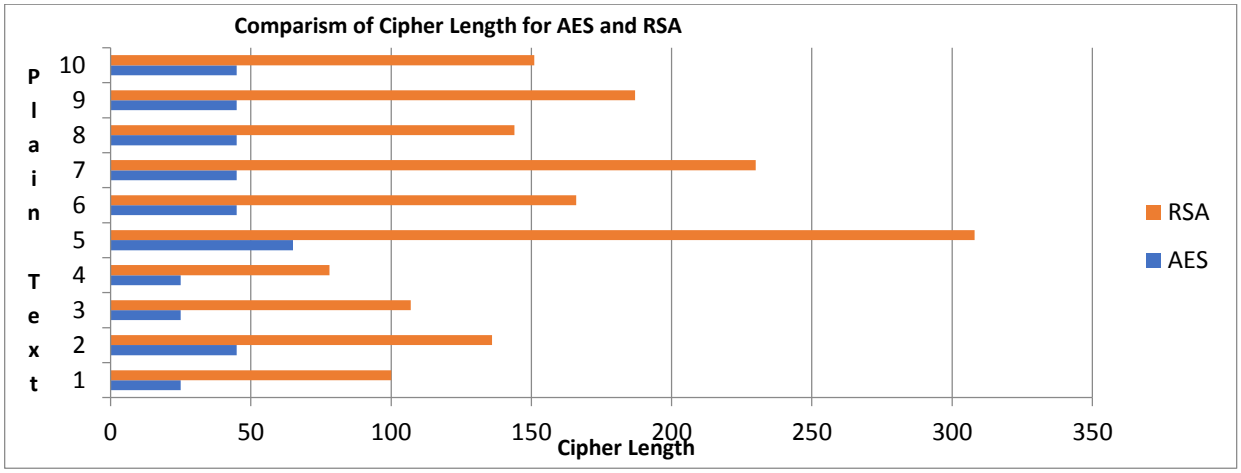

Figure 2: Comparison of AES and RSA in terms of Cipher length

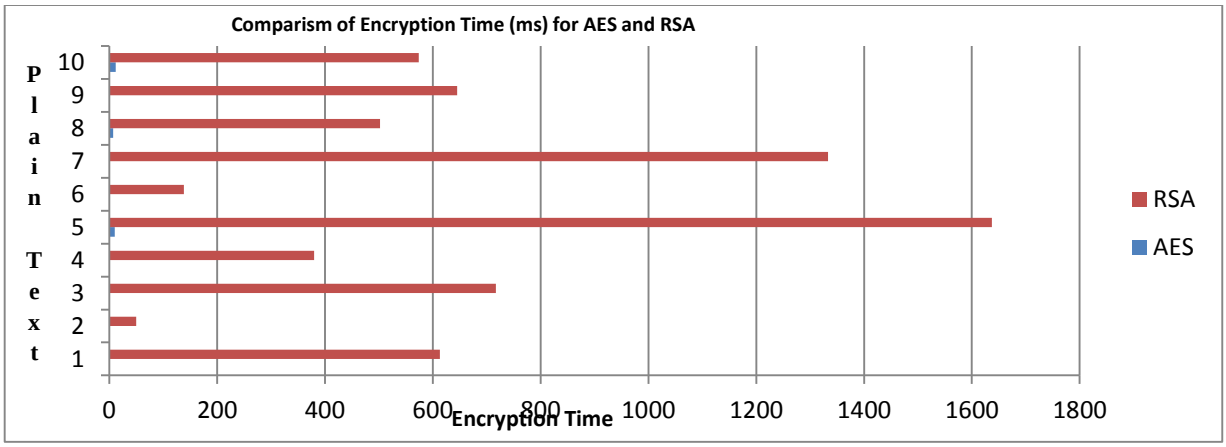

Figure 3: Comparison of AES and RSA in terms of encryption time

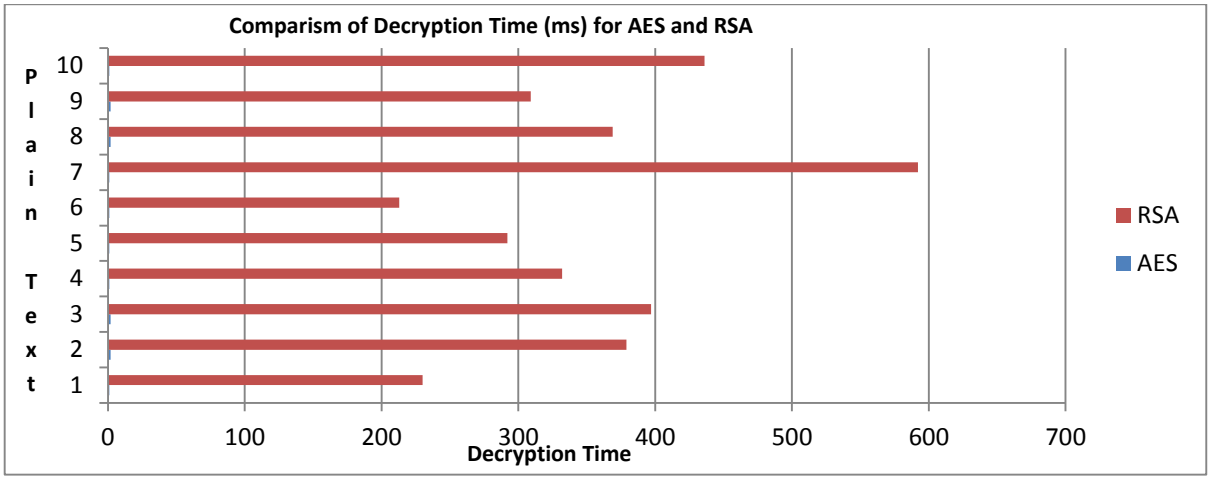

Figure 4: Comparison of AES and RSA in terms of decryption time

5.0 CONCLUSION

A symmetric block encryption algorithm (Advanced Encryption Standard) and an Asymmetric block encryption algorithm (Rivest Shamir Algorithm) were compared to test their performances in terms of encryption time, decryption time, cipher length, and key length. The result shows that AES is better between the two encryption techniques. The author is recommending AES as a good algorithm for security measure especially in the development of mobile applications.

REFERENCE

Adolf, F., Joseph, G. & Kwabena, R. (2014) Comparative Analysis of Advanced Encryption Standard, Blowfish, and Rivest Cipher 4 Algorithms. *Journal of Innovative Research and Development*. Vol. 3, Issue 11.

Agbelusi, O. (2019). Development of a Secured Framework for Societal Health Inclusion using Mobile Devices. Published Ph.D. Thesis Submitted to Department of Computer Science, Federal University of Technology, Akure, Nigeria.

Elminaam, D.S, Kader, H.M and Hadhoud, M.M (2008) "Performance Evaluation of Symmetric Encryption Algorithms", *International Journal of Computer Science and Network Security*, Vol.8 No.12, pp. 280-286.

Mandal, A.K, Parakash, C and Tiwari, A (2012) "Performance Evaluation of Cryptographic Algorithms: DES and AES" *IEEE Students' Conference on Electrical, Electronics and Computer Science*, pp. 15.

Mansoor, E., Shujaat, K. and Umer, B. (2013). Symmetric Algorithm Survey: A Comparative Analysis. *International Journal of Computer Applications.* 61(20)

Meena1, M & Komathi, A. (2013) Study and Comparative Analysis of Cryptographic Algorithms for Various File Formats. *International Journal of Science and Research* (IJSR). Volume 5 Issue 8.

Pavithra, S. and Ramade, E. (2012) "Performance Evaluation of Symmetric Algorithms", *Journal of Global Research in Computer Science*, Volume 3, No. 8, pp. 43

Nureni & Sayyidina (2018). Comparative Analysis of Encryption Algorithms. Covenant Journal of Informatics & Communication Technology. Vol. 6 No1

Seth, S.M, Rajan Ishra, R (2011) "Comparative Analysis of Encryption Algorithms for Data Communication". *International Journal of Computer Science and Technology*. Vol. 2, Issue 2, pp. 292-294

Singh & Supriya (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security *International Journal of Computer Applications*, Vol. 67, pp: 33 – 38